PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-005641
(43)Date of publication of application : 08.01.2003

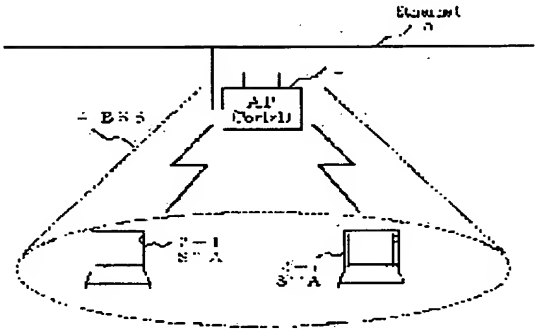
(51)Int.Cl. G09C 1/00
H04L 9/08
H04L 12/28

(21)Application number : 2001-191559
(22)Date of filing : 25.06.2001

(71)Applicant : NEC CORP
(72)Inventor : SHIMIZU MEGUMI

(54) METHOD AND APPARATUS FOR AUTHENTICATION IN WIRELESS LAN SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method and an apparatus for authentication in a wireless LAN system which can concurrently achieve delivery of an encryption key for maintaining concealment between only parties performing wireless communication and an authenticating procedure and can simplify each authenticating procedure to the same AP (a base station) performed by a S TA (a mobile terminal) completing initial authentication after releasing the authentication.
SOLUTION: The STA searches whether a MAC address of the AP intending to perform the wireless communication exists in an AP information managing table maintained by the STA. If the MAC address does not exist in the AP information managing table, a request for authenticating a public key is transmitted to the AP. If the MAC address exists in the AP information managing table, a request for re-authenticating the public key is transmitted to the AP.



LEGAL STATUS

[Date of request for examination] 28.05.2002
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3702812
[Date of registration] 29.07.2005
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－5641
（P2003－5641A）
(43)公開日　平成15年1月8日(2003.1.8)

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
G09C 1/00	640	G09C 1/00	640Z	5J104
H04L 9/08		H04L 12/28	300Z	5K033
12/28	300	9/00	601C	
			601E	

審査請求 有　請求項の数16 OL （全 13 頁）

(21)出願番号　特願2001－191559(P2001－191559)

(22)出願日　平成13年6月25日(2001.6.25)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

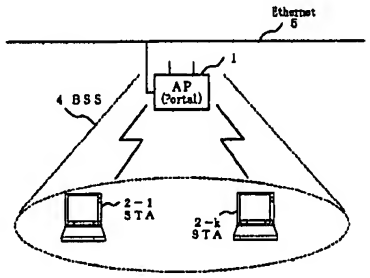
(72)発明者　清水　めぐみ
東京都港区芝五丁目７番１号　日本電気株式会社内

(74)代理人　100082935
弁理士　京本　直樹　（外２名）

Ｆターム(参考)　5J104 AA07 AA16 EA06 EA19 KA02 KA05 KA06 NA02 NA20
5K033 AA08 CC02 DA01 DA19

(54)【発明の名称】　無線ＬＡＮシステムにおける認証方法と認証装置

(57)【要約】
【課題】無線通信を行う当事者間でのみ秘匿性を保持した暗号用の鍵配送と認証手順の同時実現を可能とすると共に、初回の認証を完了したＳＴＡ（移動端末局）に関しては、認証解除後の同一ＡＰ（基地局）に対する２回目以降の認証手順の簡略化を実現可能とする、無線ＬＡＮシステムにおける認証方法と認証装置を提供する。
【解決手段】ＳＴＡは、無線通信を行おうとするＡＰのＭＡＣアドレスがＳＴＡの保持するＡＰ情報管理テーブル内に存在するか否かを検索し、前記ＭＡＣアドレスが前記ＡＰ情報管理テーブル内に存在しない場合には、前記ＡＰに対して公開鍵認証要求を行い、前記ＭＡＣアドレスが前記ＡＰ情報管理テーブル内に存在する場合には、前記ＡＰに対して公開鍵再認証要求を行うことを特徴とする。



【特許請求の範囲】
【請求項１】　無線ＬＡＮシステムにおける認証方法において、ＳＴＡ（移動端末局）は、無線通信を行おうとするＡＰ（基地局）のＭＡＣアドレスが前記ＳＴＡの保持するＡＰ情報管理テーブル内に存在するか否かを検索し、前記ＭＡＣアドレスが前記ＡＰ情報管理テーブル内に存在しない場合には、前記ＳＴＡは前記ＡＰに対して公開鍵認証要求を行い、前記ＡＰは前記公開鍵認証要求が妥当である場合には前記ＳＴＡの認証を行い、前記ＭＡＣアドレスが前記ＡＰ情報管理テーブル内に存在する場合には、前記ＳＴＡは前記ＡＰに対して公開鍵再認証要求を行い、前記ＡＰは前記公開鍵再認証要求が妥当である場合には前記ＳＴＡの認証を行う、ことを特徴とする無線ＬＡＮシステムにおける認証方法。
【請求項２】　前記ＡＰ情報管理テーブルは、前記ＳＴＡが前記公開鍵認証要求を行って該公開鍵認証の完了実績のあるＡＰのＭＡＣアドレスを最新認証完了実績順に保持することを特徴とする請求項１に記載の無線ＬＡＮシステムにおける認証方法。
【請求項３】　前記ＡＰは、自らの秘密鍵であるＡＰ秘密鍵と、前記ＡＰ秘密鍵に対応する公開鍵であるところのＡＰ公開鍵と、前記ＡＰ公開鍵を付した自らのユーザ証明書であるところのＡＰユーザ証明書とを保持し、前記ＳＴＡは、自らの秘密鍵であるＳＴＡ秘密鍵と、前記ＳＴＡ秘密鍵に対応する公開鍵であるところのＳＴＡ公開鍵と、前記ＳＴＡ公開鍵を付した自らのユーザ証明書であるところのＳＴＡユーザ証明書とを保持している、ことを特徴とする請求項１或いは請求項２の何れか１項に記載の無線ＬＡＮシステムにおける認証方法。
【請求項４】　前記ＳＴＡが前記ＡＰに対して前記公開鍵認証要求を行うステップは、公開鍵認証手順によって構成され、前記公開鍵認証手順は、前記ＳＴＡから前記ＡＰに対して認証要求を行うステップと、前記認証要求を受信した前記ＡＰから前記ＳＴＡに対して前記ＡＰユーザ証明書を送信するステップと、前記ＡＰユーザ証明書を受信した前記ＳＴＡが、前記ＡＰユーザ証明書を検証した後に前記ＡＰユーザ証明書に添付された前記ＡＰ公開鍵を用いて前記ＳＴＡユーザ証明書を暗号化して暗号化ＳＴＡユーザ証明書を作成し、前記暗号化ＳＴＡユーザ証明書を前記ＡＰに対して送信するステップと、前記暗号化ＳＴＡユーザ証明書を受信した前記ＡＰが、前記暗号化ＳＴＡユーザ証明書を前記ＡＰ秘密鍵で復号化して前記ＳＴＡユーザ証明書を再生し、前記ＳＴＡユーザ証明書を検証した後に前記ＳＴＡユーザ証明書に添付された前記ＳＴＡ公開鍵を用いて前記ＡＰが生成した共通鍵を暗号化して暗号化共通鍵を作成し、前記暗号化共通鍵を前記ＳＴＡに送信して認証許可を通知するステップとから構成され、前記暗号化共通鍵を受信した前記ＳＴＡが、前記暗号化共通鍵を前記ＳＴＡ秘密鍵で復号化して前記共通鍵を再生し、以降のフレーム暗号化通信に該共通鍵を使用する、ことを特徴とする請求項３に記載の無線ＬＡＮシステムにおける認証方法。
【請求項５】　前記ＳＴＡが前記ＡＰに対して前記公開鍵認証要求を行う際に送受信されるＭＡＣフレーム内のフレームボディ部のAlgorithm Numberの値は、「０」又は「１」でない任意の数「ｎ」である、ことを特徴とする請求項４に記載の無線ＬＡＮシステムにおける認証方法。
【請求項６】　前記ＡＰは公開鍵管理テーブルを保持し、前記公開鍵管理テーブルは前記ＡＰが過去に認証許可を通知した実績の有る前記ＳＴＡのＭＡＣアドレスと、該ＳＴＡの前記ＳＴＡ公開鍵と、前記ＡＰが該ＳＴＡの認証許可時に生成し発行した共通鍵とを、最新認証許可順に保持する、ことを特徴とする請求項５に記載の無線ＬＡＮシステムにおける認証方法。
【請求項７】　前記ＳＴＡが前記ＡＰに対して前記公開鍵再認証要求を行うステップは、公開鍵再認証手順によって構成され、前記公開鍵再認証手順は、前記ＳＴＡから前記ＡＰに対して再認証要求を行うステップと、前記再認証要求を受信した前記ＡＰが、前記公開鍵再認証要求を送信した前記ＳＴＡのＭＡＣアドレスが前記ＡＰの保持する前記公開鍵管理テーブル内に存在するか検索し、検索した結果、前記ＳＴＡのＭＡＣアドレスが前記公開鍵管理テーブルに存在し、かつ、該ＭＡＣアドレスに対応する公開鍵であるところの前記ＳＴＡ公開鍵を前記公開鍵管理テーブル内に保持していることを確認した場合には、前記ＡＰは、当該ＳＴＡに対して指定する新たな共通鍵である新共通鍵を生成し、該新共通鍵を前記ＳＴＡ公開鍵で暗号化して暗号化新共通鍵を生成し、該暗号化新共通鍵を前記ＳＴＡに送信して認証許可を通知するステップとから構成され、前記暗号化新共通鍵を受信した前記ＳＴＡが、前記暗号化新共通鍵を前記ＳＴＡ秘密鍵で復号化して前記新共通鍵を再生し、以降のフレーム暗号化通信に該新共通鍵を使用する、ことを特徴とする請求項６に記載の無線ＬＡＮシステムにおける認証方法。
【請求項８】　前記ＳＴＡが前記ＡＰに対して前記公開鍵再認証要求を行う際に送受信されるＭＡＣフレーム内のフレームボディ部のAlgorithm Numberの値は、「０」と「１」と「ｎ」でない任意の数「ｍ」である、ことを特徴とする請求項７に記載の無線ＬＡＮシステムにおける認証方法。
【請求項９】　無線ＬＡＮシステムにおける認証装置において、無線通信を行おうとするＡＰ（基地局）のＭＡＣアドレスが自身の保持するＡＰ情報管理テーブル内に存在するか否かを検索し、前記ＭＡＣアドレスが前記ＡＰ情報管理テーブル内に存在しない場合には、前記ＡＰに対して公開鍵認証要求を行い、前記ＭＡＣアドレスが前記ＡＰ情報管理テーブル内に存在する場合には、前記ＡＰに対して公開鍵再認証要求を行うＳＴＡ（移動端末

局）と、前記ＳＴＡからの前記公開鍵認証要求あるいは前記公開鍵再認証要求が妥当である場合には前記ＳＴＡの認証を行う前記ＡＰと、を備えることを特徴とする無線ＬＡＮシステムにおける認証装置。

【請求項１０】　前記ＡＰ情報管理テーブルは、前記ＳＴＡが前記公開鍵認証要求を行って該公開鍵認証の完了実績の有るＡＰのＭＡＣアドレスを最新認証完了実績順に保持することを特徴とする請求項９に記載の無線ＬＡＮシステムにおける認証装置。

【請求項１１】　前記ＡＰは、自らの秘密鍵であるＡＰ秘密鍵と、前記ＡＰ秘密鍵に対応する公開鍵であるところのＡＰ公開鍵と、前記ＡＰ公開鍵を付した自らのユーザ証明書であるところのＡＰユーザ証明書とを保持し、前記ＳＴＡは、自らの秘密鍵であるＳＴＡ秘密鍵と、前記ＳＴＡ秘密鍵に対応する公開鍵であるところのＳＴＡ公開鍵と、前記ＳＴＡ公開鍵を付した自らのユーザ証明書であるところのＳＴＡユーザ証明書とを保持している、ことを特徴とする請求項９或いは請求項１０の何れか１項に記載の無線ＬＡＮシステムにおける認証装置。

【請求項１２】　前記ＳＴＡが前記ＡＰに対して前記公開鍵認証要求を行う場合には、前記ＳＴＡから前記ＡＰに対して認証要求を行い、前記認証要求を受信した前記ＡＰから前記ＳＴＡに対して前記ＡＰユーザ証明書を送信し、前記ＡＰユーザ証明書を受信した前記ＳＴＡが、前記ＡＰユーザ証明書を検証した後に前記ＡＰユーザ証明書に添付された前記ＡＰ公開鍵を用いて前記ＳＴＡユーザ証明書を暗号化して暗号化ＳＴＡユーザ証明書を作成し、前記暗号化ＳＴＡユーザ証明書を前記ＡＰに対して送信し、前記暗号化ＳＴＡユーザ証明書を受信した前記ＡＰが、前記暗号化ＳＴＡユーザ証明書を前記ＡＰ秘密鍵で復号化して前記ＳＴＡユーザ証明書を再生し、前記ＳＴＡユーザ証明書を検証した後に前記ＳＴＡユーザ証明書に添付された前記ＳＴＡ公開鍵を用いて前記ＡＰが生成した共通鍵を暗号化して暗号化共通鍵を作成し、前記暗号化共通鍵を前記ＳＴＡに送信して認証許可を通知し、前記暗号化共通鍵を受信した前記ＳＴＡが、前記暗号化共通鍵を前記ＳＴＡ秘密鍵で復号化して前記共通鍵を再生し、以降のフレーム暗号化通信に該共通鍵を使用する、ことを特徴とする請求項１１に記載の無線ＬＡＮシステムにおける認証装置。

【請求項１３】　前記ＳＴＡが前記ＡＰに対して前記公開鍵認証要求を行う際に送受信されるＭＡＣフレーム内のフレームボディ部のAlgorithm Numberの値は、「０」又は「１」でない任意の数「ｎ」である、ことを特徴とする請求項１２に記載の無線ＬＡＮシステムにおける認証装置。

【請求項１４】　前記ＡＰは公開鍵管理テーブルを保持し、前記公開鍵管理テーブルは前記ＡＰが過去に認証許可を通知した実績の有る前記ＳＴＡのＭＡＣアドレスと、該ＳＴＡの前記ＳＴＡ公開鍵と、前記ＡＰが該ＳＴＡの認証許可時に生成し発行した共通鍵とを、最新認証許可順に保持する、ことを特徴とする請求項１３に記載の無線ＬＡＮシステムにおける認証装置。

【請求項１５】　前記ＳＴＡが前記ＡＰに対して前記公開鍵再認証要求を行う場合には、前記ＳＴＡから前記ＡＰに対して再認証要求を行い、前記再認証要求を受信した前記ＡＰが、前記公開鍵再認証要求を送信した前記ＳＴＡのＭＡＣアドレスが前記ＡＰの保持する前記公開鍵管理テーブル内に存在するか検索し、検索した結果、前記ＳＴＡのＭＡＣアドレスが前記公開鍵管理テーブルに存在し、かつ、該ＭＡＣアドレスに対応する公開鍵であるところの前記ＳＴＡ公開鍵を前記公開鍵管理テーブル内に保持していることを確認した場合には、前記ＡＰは、当該ＳＴＡに対して指定する新たな共通鍵である新共通鍵を生成し、該新共通鍵を前記ＳＴＡ公開鍵で暗号化して暗号化新共通鍵を生成し、該暗号化新共通鍵を前記ＳＴＡに送信して認証許可を通知し、前記暗号化新共通鍵を受信した前記ＳＴＡが、前記暗号化新共通鍵を前記ＳＴＡ秘密鍵で復号化して前記新共通鍵を再生し、以降のフレーム暗号化通信に該新共通鍵を使用する、ことを特徴とする請求項１４に記載の無線ＬＡＮシステムにおける認証装置。

【請求項１６】　前記ＳＴＡが前記ＡＰに対して前記公開鍵再認証要求を行う際に送受信されるＭＡＣフレーム内のフレームボディ部のAlgorithm Numberの値は、「０」と「１」と「ｎ」でない任意の数「ｍ」である、ことを特徴とする請求項１５に記載の無線ＬＡＮシステムにおける認証装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は無線ＬＡＮシステムにおける認証方法と認証装置に関し、特にデータを暗号化して無線通信する無線ＬＡＮシステムにおいて、無線通信を行う当事者間でのみ秘匿性を保持した暗号用の鍵配送と認証の同時実現を可能とする、無線ＬＡＮシステムにおける認証方法と認証装置に関する。

【０００２】

【従来の技術】無線ＬＡＮ（Local Area Network：ラン）システムにおいては、送受信するデータの秘匿性を保持するために、送受信するデータフレームの暗号化が必須の条件となってきている。

【０００３】無線ＬＡＮシステムにおける暗号化方式については、これまでＩＥＥＥ（Institute of Electrical and Electronics Engineers：米国、電気／電子技術者協会）８０２委員会を中心として標準化の検討が進められてきており、その標準仕様であるIEEE802.11においては、無線ＬＡＮにおける無線区間の暗号化及び認証の方式の１つとして、Shared Key（共通鍵）認証方式が採用されている。

【０００４】Shared Key方式においては、図１に示すような無線ＬＡＮの基地局としてのＡＰ（Access Point：アクセスポイント）１と移動端末局としてのＳＴＡ（Station：ステーション）２とが、通信相手毎に互いに保持することのできる１種類の共通鍵を使用する、又は１種類の共通鍵を保持していない場合には、両者共通の鍵情報として４種類の共通鍵を保持しておき、フレーム暗号化通信を行う際には４種類の共通鍵の中の１つの共通鍵を選択して使用するようになっている。しかし、暗号化用の鍵の配送方法に関しては、IEEE802.11には定義されておらず、実装依存となっている。

【０００５】Shared Key方式における認証手順について、図１０及び図１１を参照して説明する。

【０００６】図１０は、Shared Key方式における認証手順を示す図であり、図１１は、Shared Key方式の認証手順において送受信されるフレームフォーマットのフレームボディ部を示す図である。

【０００７】図１０において、ＡＰ１に対してShared Key方式による認証要求を行うＳＴＡ２は、ＡＰ１に対して認証フレーム１を送信する（ステップＳ１）。認証フレーム１のフレームボディ部は、図１１の（１）認証フレーム１に示す形式となっており、Algorithm Number（アルゴリズム番号）１１－１－１を「１」とし、Transaction Sequence Number（トランザクションシーケンス番号）１１－１－２を「１」としたフレームとなっている。なお、Shared Key方式における認証時には、Algorithm Number１１－１－１～１１－４－１は常に「１」であると定義されている。

【０００８】ステップＳ１でＳＴＡ２から認証要求を受信したＡＰ１は、認証フレーム２を用いてChallenge Text（チャレンジテキスト）というランダムなビット列をＳＴＡ２に対して送信する（ステップＳ２）。認証フレーム２は、図１１の（２）認証フレーム２に示す形式となっており、Algorithm Number１１－２－１は前述の通り「１」であり、Transaction Sequence Number １１－２－２は「２」で、Challenge Text element（チャレンジテキストエレメント）１１－２－４にChallenge Textを挿入したフレームとなっている。

【０００９】ステップＳ２でＡＰ１から認証フレーム２を受信したＳＴＡ２は、ＡＰ１から受信したChallenge Textと、該Challenge Textに対するCRC32(Cyclic Redundancy Code 32bits)算出結果に相当するICV（Integrity Check Value：インテグリティチェックバリュー）に対して、共通鍵の１つで暗号化を行う（ステップＳ３）。そして、暗号化したChallenge TextとICVを、使用した共通鍵の鍵情報であるIV（Initialization Vector：イニシャライゼイション・ベクター）と共に、認証フレーム３を用いてＡＰ１に対して送信する（ステップＳ４）。認証フレーム３は、図１１の（３）認証フレーム３に示す形式となっており、Algorithm Number１１－３－１は前述の通り「１」であり、Transaction Sequence Number １１－３－２は「３」で、IV１１－３－３、Challenge Text element（暗号化したChallenge Text）１１－３－４、ICV １１－３－５を付加したフレームとなっている。

【００１０】ステップＳ４で認証フレーム３を受信したＡＰ１は、受信フレーム内鍵情報（IV１１－３－３）からそれに対応する共通鍵を用いて受信フレームの暗号化部を復号化し、受信フレーム内ICV（ICV １１－３－５）と復号結果から算出したICVの一致と、復号結果から得られる平文とステップＳ２で送信したChallenge Textとの一致を確認した場合には（ステップＳ５で一致を確認した場合）、認証フレーム４をＳＴＡ２に対して送信して認証完了を通知する（ステップＳ６）。認証フレーム４は、図１１の（４）認証フレーム４に示す形式となっており、Algorithm Number１１－４－１は前述の通り「１」であり、Transaction Sequence Number １１－４－２は「４」で、Status Code（ステータスコード）１１－４－９を付加したフレームとなっている。なお、図１１に示したStatus Code １１－１－９、Status Code １１－２－９、Status Code １１－３－９及びStatus Code １１－４－９は、フレーム受信成功の可否などを通信相手に通知するための情報フィールドである。

【００１１】以上の動作により、Shared Key方式における認証手順が終了し、以後、ＳＴＡ２とＡＰ１間で共通鍵を用いたフレーム暗号化通信が行われるようになっている。

【００１２】Shared Key方式における認証と鍵配送の方法には、様々な手法が多数提案されており、例えばその１つとして、通信を行う当事者以外の第三者（例えば鍵管理サーバ）を介在させる手法や、他の１つとして、通信を行う当事者間でのみ秘密情報の交換を行う手法がある。前者の一例としては、特開２００１－１１１５４４号公報記載の「無線ＬＡＮシステムにおける認証方法と認証装置」が知られており、この公報では、認証サーバと、何らかの方法で予め配布し保持させた共通鍵を用いて、暗号化認証を行う技術が記載されている。また、後者の一例としては、特開平１１－１９１７６１号公報記載の「相互認証方法及びその装置」が知られており、この公報では、Diffie-Hellmanの鍵配送アルゴリズムを用いて公開鍵の正当性を確認する技術が記載されている。

【００１３】

【発明が解決しようとする課題】第１の例として上述した鍵管理サーバを利用したシステムでは、予め移動端末局の情報を鍵管理サーバに登録しておくものであり、鍵配送手順と認証手順が分離されることにより、暗号化を伴う認証手順が複雑なものとなるという欠点を有している。

【００１４】また、第２の例として上述した鍵配送アルゴリズムを用いた認証手順においては、通信を行う当事者間でのみ秘匿性を保持した鍵配送と認証を同時に行う

ことが可能となるが、その認証手順が複雑となり演算に多くの時間を要するものとなっており、無線伝播環境の問題などによって通信が絶たれた際の認証解除時における再度の認証手順実行時にも、初回の認証時と同一手順を踏むこととなり、本来のデータ通信以外のオーバーヘッドトラヒックを増大させてしまうという欠点を有している。

【００１５】本発明は上述した事情を改善するためになされたものであり、本発明の目的は、無線通信を行う当事者間でのみ秘匿性を保持した暗号用の鍵配送と認証手順の同時実現を可能とすると共に、初回の認証を完了したＳＴＡ（移動端末局）に関しては、認証解除後の同一ＡＰ（基地局）に対する２回目以降の認証手順の簡略化を実現可能とする、無線ＬＡＮシステムにおける認証方法と認証装置を提供することにある。

【００１６】

【課題を解決するための手段】本発明の無線ＬＡＮシステムにおける認証方法は、無線ＬＡＮシステムにおける認証方法において、ＳＴＡ（移動端末局）は、無線通信を行おうとするＡＰ（基地局）のＭＡＣアドレスが前記ＳＴＡの保持するＡＰ情報管理テーブル内に存在するか否かを検索し、前記ＭＡＣアドレスが前記ＡＰ情報管理テーブル内に存在しない場合には、前記ＳＴＡは前記ＡＰに対して公開鍵認証要求を行い、前記ＡＰは前記公開鍵認証要求が妥当である場合には前記ＳＴＡの認証を行い、前記ＭＡＣアドレスが前記ＡＰ情報管理テーブル内に存在する場合には、前記ＳＴＡは前記ＡＰに対して公開鍵再認証要求を行い、前記ＡＰは前記公開鍵再認証要求が妥当である場合には前記ＳＴＡの認証を行う、ことを特徴とする。

【００１７】また、前記ＡＰ情報管理テーブルは、前記ＳＴＡが前記公開鍵認証要求を行って該公開鍵認証の完了実績のあるＡＰのＭＡＣアドレスを最新認証完了実績順に保持することを特徴とする。

【００１８】さらに、前記ＡＰは、自らの秘密鍵であるＡＰ秘密鍵と、前記ＡＰ秘密鍵に対応する公開鍵であるところのＡＰ公開鍵と、前記ＡＰ公開鍵を付した自らのユーザ証明書であるところのＡＰユーザ証明書とを保持し、前記ＳＴＡは、自らの秘密鍵であるＳＴＡ秘密鍵と、前記ＳＴＡ秘密鍵に対応する公開鍵であるところのＳＴＡ公開鍵と、前記ＳＴＡ公開鍵を付した自らのユーザ証明書であるところのＳＴＡユーザ証明書とを保持している、ことを特徴とする。

【００１９】また、前記ＳＴＡが前記ＡＰに対して前記公開鍵認証要求を行うステップは、公開鍵認証手順によって構成され、前記公開鍵認証手順は、前記ＳＴＡから前記ＡＰに対して認証要求を行うステップと、前記認証要求を受信した前記ＡＰから前記ＳＴＡに対して前記ＡＰユーザ証明書を送信するステップと、前記ＡＰユーザ証明書を受信した前記ＳＴＡが、前記ＡＰユーザ証明書を検証した後に前記ＡＰユーザ証明書に添付された前記ＡＰ公開鍵を用いて前記ＳＴＡユーザ証明書を暗号化して暗号化ＳＴＡユーザ証明書を作成し、前記暗号化ＳＴＡユーザ証明書を前記ＡＰに対して送信するステップと、前記暗号化ＳＴＡユーザ証明書を受信した前記ＡＰが、前記暗号化ＳＴＡユーザ証明書を前記ＡＰ秘密鍵で復号化して前記ＳＴＡユーザ証明書を再生し、前記ＳＴＡユーザ証明書を検証した後に前記ＳＴＡユーザ証明書に添付された前記ＳＴＡ公開鍵を用いて前記ＡＰが生成した共通鍵を暗号化して暗号化共通鍵を作成し、前記暗号化共通鍵を前記ＳＴＡに送信して認証許可を通知するステップとから構成され、前記暗号化共通鍵を受信した前記ＳＴＡが、前記暗号化共通鍵を前記ＳＴＡ秘密鍵で復号化して前記共通鍵を再生し、以降のフレーム暗号化通信に該共通鍵を使用する、ことを特徴とする。

【００２０】さらに、前記ＳＴＡが前記ＡＰに対して前記公開鍵認証要求を行う際に送受信されるＭＡＣフレーム内のフレームボディ部のAlgorithm Numberの値は、「０」又は「１」でない任意の数「ｎ」である、ことを特徴とする。

【００２１】また、前記ＡＰは公開鍵管理テーブルを保持し、前記公開鍵管理テーブルは前記ＡＰが過去に認証許可を通知した実績の有る前記ＳＴＡのＭＡＣアドレスと、該ＳＴＡの前記ＳＴＡ公開鍵と、前記ＡＰが該ＳＴＡの認証許可時に生成し発行した共通鍵とを、最新認証許可順に保持する、ことを特徴とする。

【００２２】さらに、前記ＳＴＡが前記ＡＰに対して前記公開鍵再認証要求を行うステップは、公開鍵再認証手順によって構成され、前記公開鍵再認証手順は、前記ＳＴＡから前記ＡＰに対して再認証要求を行うステップと、前記再認証要求を受信した前記ＡＰが、前記公開鍵再認証要求を送信した前記ＳＴＡのＭＡＣアドレスが前記ＡＰの保持する前記公開鍵管理テーブル内に存在するか検索し、検索した結果、前記ＳＴＡのＭＡＣアドレスが前記公開鍵管理テーブルに存在し、かつ、該ＭＡＣアドレスに対応する公開鍵であるところの前記ＳＴＡ公開鍵を前記公開鍵管理テーブル内に保持していることを確認した場合には、前記ＡＰは、当該ＳＴＡに対して指定する新たな共通鍵である新共通鍵を生成し、該新共通鍵を前記ＳＴＡ公開鍵で暗号化して暗号化新共通鍵を生成し、該暗号化新共通鍵を前記ＳＴＡに送信して認証許可を通知するステップとから構成され、前記暗号化新共通鍵を受信した前記ＳＴＡが、前記暗号化新共通鍵を前記ＳＴＡ秘密鍵で復号化して前記新共通鍵を再生し、以降のフレーム暗号化通信に該新共通鍵を使用する、ことを特徴とする。

【００２３】また、前記ＳＴＡが前記ＡＰに対して前記公開鍵再認証要求を行う際に送受信されるＭＡＣフレーム内のフレームボディ部のAlgorithm Numberの値は、「０」と「１」と「ｎ」でない任意の数「ｍ」である、

ことを特徴とする。

【００２４】本発明の無線ＬＡＮシステムにおける認証装置は、無線ＬＡＮシステムにおける認証装置において、無線通信を行おうとするＡＰ（基地局）のＭＡＣアドレスが自身の保持するＡＰ情報管理テーブル内に存在するか否かを検索し、前記ＭＡＣアドレスが前記ＡＰ情報管理テーブル内に存在しない場合には、前記ＡＰに対して公開鍵認証要求を行い、前記ＭＡＣアドレスが前記ＡＰ情報管理テーブル内に存在する場合には、前記ＡＰに対して公開鍵再認証要求を行うＳＴＡ（移動端末局）と、前記ＳＴＡからの前記公開鍵認証要求あるいは前記公開鍵再認証要求が妥当である場合には前記ＳＴＡの認証を行う前記ＡＰと、を備えることを特徴とする。

【００２５】また、前記ＡＰ情報管理テーブルは、前記ＳＴＡが前記公開鍵認証要求を行って該公開鍵認証の完了実績のあるＡＰのＭＡＣアドレスを最新認証完了実績順に保持することを特徴とする。

【００２６】さらに、前記ＡＰは、自らの秘密鍵であるＡＰ秘密鍵と、前記ＡＰ秘密鍵に対応する公開鍵であるところのＡＰ公開鍵と、前記ＡＰ公開鍵を付した自らのユーザ証明書であるところのＡＰユーザ証明書とを保持し、前記ＳＴＡは、自らの秘密鍵であるＳＴＡ秘密鍵と、前記ＳＴＡ秘密鍵に対応する公開鍵であるところのＳＴＡ公開鍵と、前記ＳＴＡ公開鍵を付した自らのユーザ証明書であるところのＳＴＡユーザ証明書とを保持している、ことを特徴とする。

【００２７】また、前記ＳＴＡが前記ＡＰに対して前記公開鍵認証要求を行う場合には、前記ＳＴＡから前記ＡＰに対して認証要求を行い、前記認証要求を受信した前記ＡＰから前記ＳＴＡに対して前記ＡＰユーザ証明書を送信し、前記ＡＰユーザ証明書を受信した前記ＳＴＡが、前記ＡＰユーザ証明書を検証した後に前記ＡＰユーザ証明書に添付された前記ＡＰ公開鍵を用いて前記ＳＴＡユーザ証明書を暗号化して暗号化ＳＴＡユーザ証明書を作成し、前記暗号化ＳＴＡユーザ証明書を前記ＡＰに対して送信し、前記暗号化ＳＴＡユーザ証明書を受信した前記ＡＰが、前記暗号化ＳＴＡユーザ証明書を前記ＡＰ秘密鍵で復号化して前記ＳＴＡユーザ証明書を再生し、前記ＳＴＡユーザ証明書を検証した後に前記ＳＴＡユーザ証明書に添付された前記ＳＴＡ公開鍵を用いて前記ＡＰが生成した共通鍵を暗号化して暗号化共通鍵を作成し、前記暗号化共通鍵を前記ＳＴＡに送信して認証許可を通知し、前記暗号化共通鍵を受信した前記ＳＴＡが、前記暗号化共通鍵を前記ＳＴＡ秘密鍵で復号化して前記共通鍵を再生し、以降のフレーム暗号化通信に該共通鍵を使用する、ことを特徴とする。

【００２８】さらに、前記ＳＴＡが前記ＡＰに対して前記公開鍵認証要求を行う際に送受信されるＭＡＣフレーム内のフレームボディ部のAlgorithm Numberの値は、「０」又は「１」でない任意の数「ｎ」である、ことを特徴とする。

【００２９】また、前記ＡＰは公開鍵管理テーブルを保持し、前記公開鍵管理テーブルは前記ＡＰが過去に認証許可を通知した実績の有る前記ＳＴＡのＭＡＣアドレスと、該ＳＴＡの前記ＳＴＡ公開鍵と、前記ＡＰが該ＳＴＡの認証許可時に生成し発行した共通鍵とを、最新認証許可順に保持する、ことを特徴とする。

【００３０】さらに、前記ＳＴＡが前記ＡＰに対して前記公開鍵再認証要求を行う場合には、前記ＳＴＡから前記ＡＰに対して再認証要求を行い、前記再認証要求を受信した前記ＡＰが、前記公開鍵再認証要求を送信した前記ＳＴＡのＭＡＣアドレスが前記ＡＰの保持する前記公開鍵管理テーブル内に存在するか検索し、検索した結果、前記ＳＴＡのＭＡＣアドレスが前記公開鍵管理テーブルに存在し、かつ、該ＭＡＣアドレスに対応する公開鍵であるところの前記ＳＴＡ公開鍵を前記公開鍵管理テーブル内に保持していることを確認した場合には、前記ＡＰは、当該ＳＴＡに対して指定する新たな共通鍵である新共通鍵を生成し、該新共通鍵を前記ＳＴＡ公開鍵で暗号化して暗号化新共通鍵を生成し、該暗号化新共通鍵を前記ＳＴＡに送信して認証許可を通知し、前記暗号化新共通鍵を受信した前記ＳＴＡが、前記暗号化新共通鍵を前記ＳＴＡ秘密鍵で復号化して前記新共通鍵を再生し、以降のフレーム暗号化通信に該新共通鍵を使用する、ことを特徴とする。

【００３１】また、前記ＳＴＡが前記ＡＰに対して前記公開鍵再認証要求を行う際に送受信されるＭＡＣフレーム内のフレームボディ部のAlgorithm Numberの値は、「０」と「１」と「ｎ」でない任意の数「ｍ」である、ことを特徴とする。

【００３２】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【００３３】図１は本発明の無線ＬＡＮシステムにおける認証装置の一実施形態を示すブロック図である。

【００３４】図１に示す本実施の形態は、無線ＬＡＮの基地局としてのＡＰ（Access Point：アクセスポイント）１と、ＡＰ１に帰属する移動端末局としての複数のＳＴＡ（Station：ステーション）２（ＳＴＡ２－１、ＳＴＡ２－ｋ）とから構成されている。図１に示す実施の形態は、IEEE802.11で定義するところのInfrastructure（インフラストラクチャ）方式であり、このような無線ＬＡＮネットワークの最小単位をＢＳＳ（Basic Service Set：基本サービス・セット）４と言う。

【００３５】ＢＳＳ４内におけるＡＰ１は、各ＳＴＡ２がＡＰ１に同期するための情報を含むBeacon（ビーコン）フレームを、周期的にＢＳＳ４内にブロードキャスト送信し、当該Beaconフレームを受信したＢＳＳ４内の各ＳＴＡ２は、通信開始時にＡＰ１に対して認証要求を行い、ＡＰ１により認証許可を受けた後、ＡＰ１への帰

属処理を完了することにより、ＡＰ１との通信を行うことが可能となる。また、Infrastructure方式におけるＢＳＳ４内の各ＳＴＡ２は、ＳＴＡ２間通信時においてもＡＰ１を介した通信を行う。

【００３６】また、図１におけるＡＰ１は（portal）となっているが、Portalとは、IEEE802.11以外のＬＡＮプロトコルとのプロトコル変換機能をＡＰ１に付加したことを示しており、基地局としてのＡＰ１とＥｔｈｅｒｎｅｔ（登録商標）（イーサネット（登録商標））５などの有線ＬＡＮとの接続を可能にした基地局であることを示している。

【００３７】なお、図１に示した実施の形態は、IEEE802.11に準拠したものであるが、本実施の形態においては無線区間の暗号化及び認証の方式として、Shared Key方式（共通鍵認証方式）とは異なり、主として秘密鍵と公開鍵を用いた認証方式を採用している。従って、Shared Key方式と区別するために、本実施形態における認証方式を公開鍵認証方式と便宜的に呼ぶこととする。

【００３８】次に、図２を参照して、ＡＰ１とＳＴＡ２の詳細構成について説明する。

【００３９】図２は、ＡＰとＳＴＡの一例を示す詳細ブロック図である。

【００４０】図２において、上段のブロック図がＡＰ１であり、下段のブロック図がＳＴＡ２である。

【００４１】ＡＰ１は、図２に示す無線ＬＡＮカード１９－１と上位レイヤとのインターフェースであるところの上位レイヤインターフェース１７－１を介して、ＴＣＰ／ＩＰ（Transport Control Protocol/Internet Protocol）や各種アプリケーションなどの上位プロトコル処理を、基地局端末本体１８にて実現するものであり、ＳＴＡ２は、図２に示す無線ＬＡＮカード１９－２と上位レイヤとのインターフェースであるところの上位レイヤインターフェース１７－２を介して、ＡＰ１と同様な上位プロトコル処理を、ノート型パーソナルコンピュータなどの移動端末本体２０によって実現するものである。

【００４２】図２に示す無線ＬＡＮカード１９－１と無線ＬＡＮカード１９－２は、同一の構成を備える。従って、無線ＬＡＮカード１９において同一の構成要素に対応するものは、同一の参照数字または符号を付しておくものとする。

【００４３】図２に示す無線ＬＡＮカード１９（１９－１及び１９－２）は、無線区間でのフレーム送受信を行う無線機部１２と、変復調処理を行うIEEE802.11 PHY（Physical Layer：物理層）プロトコル処理部１３と、ＭＡＣ（Medium Access Control ：媒体アクセス制御）層でのアクセス制御を行うIEEE802.11 MACプロトコル処理部１４と、ＭＡＣ層での認証処理などの上位レイヤ処理を、内蔵するＣＰＵとメモリ１６によって実現する上位レイヤ処理部１５と、上位レイヤ処理部１５が使用するメモリ１６とから構成されている。

【００４４】次に、図３を参照して、ＳＴＡ２がＡＰ１に対して認証を要求する際に、ＳＴＡ２とＡＰ１間で送受信されるＭＡＣフレームについて説明する。

【００４５】図３は、認証要求時にＡＰとＳＴＡ間で送受信されるＭＡＣフレームの構成を説明する図である。

【００４６】ＳＴＡ２のＡＰ１に対する認証要求時には、図３に示すIEEE802.11のＭＡＣフレームフォーマットに従うＭＡＣフレーム３０－１が、ＡＰ１とＳＴＡ２間で交換され、ＭＡＣフレーム３０－１は、MAC Header（ＭＡＣヘッダー）３０－２と、FrameBody（フレームボディ）３０－３とFCS（Frame Check Sequence：フレームチェックシーケンス）３０－４とから構成されている。

【００４７】そして、Infrastructure方式におけるMAC Header３０－２は、各種フレームタイプや制御情報を示すFrame Control（フレームコントロール）３０－１１のフィールドと、送信先がビジーである場合に送信待機を行うための時間を定義するDuration（デュレーション）３０－１２のフィールドと、フレーム送信先アドレスを示すDA（Destination Address ：送信先アドレス）３０－１３のフィールドと、フレームの送信元アドレスを示すSA（Source Address：送信元アドレス）３０－１４のフィールドと、ＢＳＳ４の識別情報を示すBSSID ３０－１５のフィールドと、フレーム送信順を示すSequence Control（シーケンスコントロール）３０－１６のフィールドから構成される。

【００４８】フレーム送信時、図２に示すIEEE802.11 MACプロトコル処理部１４では、上位レイヤ処理部１５からの送信要求フレームを、図３に示すFrameBody ３０－３に入れてカプセル化し、送信要求情報から作成したMAC Header３０－２をFrameBody ３０－３の前に付加し、当該MAC Header３０－２とFrameBody ３０－３に対するCRC32（Cyclic Redundancy Code 32bits）算出結果を、FCS ３０－４としてFrameBody ３０－３の後ろに付加することにより、図３に示すようなIEEE802.11 MACプロトコルに従うＭＡＣフレーム３０－１への変換を行う。続いて図２に示すIEEE802.11 PHYプロトコル処理部１３では、当該ＭＡＣフレーム３０－１に対する変調処理を行い、無線機部１２を経て当該ＭＡＣフレーム３０－１を空間上に送出することにより、送信処理が完了する。

【００４９】フレーム受信時、図２に示すIEEE802.11 MACプロトコル処理部１４では、無線機部１２を経てIEEE802.11 PHYプロトコル処理部１３にて復調処理を行った結果として受信したＭＡＣフレーム３０－１に対してCRC32 の計算を行い、受信フレーム内のFCS ３０－４の値とCRC32 算出結果とが一致する場合には、MAC Header３０－２の内容の解析と受信フレームに対する処理を行い、FrameBody ３０－３の部分を上位レイヤ処理部１５へ通知する。

【００５０】次に、図４及び図５を参照して、本実施形態の重要な構成要素としての公開鍵管理テーブル及びＡＰ情報管理テーブルについて説明する。

【００５１】図４は、ＡＰが保持する公開鍵管理テーブルを説明する図であり、図５は、ＳＴＡが保持するＡＰ情報管理テーブルを説明する図である。

【００５２】ＡＰ１は、図４に示す公開鍵管理テーブル４０を、図２に示す無線ＬＡＮカード１９－１のメモリ１６内に保持している。公開鍵管理テーブル４０は、ＡＰ１が過去に本発明の公開鍵認証において認証許可を行った実績の有るＳＴＡ２のＭＡＣ層の物理アドレスであるところのＭＡＣアドレスを保持するSTA Mac Address（ＳＴＡのＭＡＣアドレス）４０－１の欄と、当該ＳＴＡ２の公開鍵を保持するPublic Key（パブリックキー）４０－２の欄と、ＡＰ１が認証許可時に当該ＳＴＡ２に対して発行した共通鍵を保持するShared Key（シェアードキー）４０－３の欄とから構成されている。そして、ＡＰ１は公開鍵管理テーブル４０の各行を、ＳＴＡ２の最新認証許可順に登録する。

【００５３】ＳＴＡ２は、図５に示すＡＰ情報管理テーブル５０を、図２に示す無線ＬＡＮカード１９－２のメモリ１６内に保持している。ＡＰ情報管理テーブル５０は、ＳＴＡ２が本発明の公開鍵認証を要求して該公開鍵認証の完了実績の有るＡＰ１のＭＡＣアドレスを保持するAP MAC Address（ＡＰのＭＡＣアドレス）５０－１の欄から構成されており、ＳＴＡ２はＡＰ情報管理テーブル５０の各行を、ＡＰ１の最新認証完了実績順に登録する。

【００５４】ＡＰ１は、図４にて説明した公開鍵管理テーブル４０への情報登録時には、登録済みのSTA MAC address ４０－１の検索を行い、既に登録済みの同一ＭＡＣアドレスが存在する場合には、登録内容の情報更新と共に公開鍵管理テーブル４０の先頭の行へ当該情報を移動する。また、本発明の公開鍵認証完了後のフレーム暗号化通信の実施毎に、ＡＰ１は公開鍵管理テーブル４０のSTA MAC address ４０－１の検索を行い、通信相手のＳＴＡ２の管理情報を公開鍵管理テーブル４０の先頭の行へ移動することにより、通信機会が新しい通信相手の管理情報ほど管理テーブル上位に位置付けることで、公開鍵管理テーブル４０が限界登録数に達し、新規情報登録が不可能となった場合には、公開鍵管理テーブル４０内で最も下位に位置する通信機会の最も古い通信相手の管理情報を削除することで対応する。

【００５５】また、ＳＴＡ２はＡＰ１と同様に、図５にて説明したＡＰ情報管理テーブル５０への情報登録時には、登録済みのAP MAC address５０－１の検索を行い、既に登録済みの同一ＭＡＣアドレスが存在する場合には、登録内容の情報更新と共にＡＰ情報管理テーブル５０の先頭の行へ当該情報を移動する。また、本発明の公開鍵認証完了後のフレーム暗号化通信の実施毎に、ＳＴＡ２はＡＰ情報管理テーブル５０のAP MAC address５０－１の検索を行い、通信相手のＡＰ１の管理情報をＡＰ情報管理テーブル５０の先頭の行へ移動することにより、通信機会が新しい通信相手の管理情報ほど管理テーブル上位に位置付けることで、ＡＰ情報管理テーブル５０が限界登録数に達し、新規情報登録が不可能となった場合には、ＡＰ情報管理テーブル５０内で最も下位に位置する通信機会の最も古い通信相手の管理情報を削除することで対応する。

【００５６】次に、図６、図７、図８、図９を参照して、本実施形態の動作について説明する。

【００５７】本実施形態においては、図１に示した無線ＬＡＮシステムの、基地局であるＡＰ１と移動端末局であるＳＴＡ２は、共に、自らの秘密鍵とそれに対応する公開鍵、及び該公開鍵を添付したユーザ証明書を保持しているものとする。そして、当該ユーザ証明書は、認証機関に代表される第三者によって、公開鍵とその保有者（すなわち、ＡＰ１或いはＳＴＡ２）との関係、及び保有者自身の正当性を証明可能である、という条件を前提とするものとする。以下では、ユーザ証明書はデジタルユーザ証明書を意味するものとする。

【００５８】図１におけるＳＴＡ２がＡＰ１を介しての無線通信を行おうとする場合には、ＳＴＡ２は先ずＡＰ１に対して、本発明の公開鍵認証要求を送信することから開始する。

【００５９】ＳＴＡ２は公開鍵認証開始時に、認証要求先のＡＰ１のＭＡＣアドレスを用いて図５に示したＡＰ情報管理テーブル５０内のAP MAC Address５０－１の検索を行い、ＡＰ情報管理テーブル５０内に認証要求先ＡＰ１のＭＡＣアドレスが存在しない場合には、初回の認証要求として図６に示す公開鍵認証手順を行い、認証要求先ＡＰ１のＭＡＣアドレスが存在する場合には、過去に当該ＡＰ１との公開鍵認証の完了実績が有る場合であるため、再認証として、図８に示す公開鍵再認証手順を行う。

【００６０】先ず、初回の認証要求としての公開鍵認証手順について、図６及び図７を参照して説明する。

【００６１】図６は、公開鍵認証手順を示す図であり、図７は、公開鍵認証手順において送受信されるＭＡＣフレームのフレームボディ部（図３のFrameBody３０－３）を示す図である。

【００６２】図６において、ＡＰ１に対して公開鍵認証手順による認証要求を行うＳＴＡ２は、ＡＰ１に対して認証フレーム６１を送信する（ステップＳ６１）。認証フレーム６１のフレームボディ部は、図７の（１）認証フレーム６１に示す形式となっており、Algorithm Number（アルゴリズム番号）７０－１－１を「n」とし、Transaction Sequence Number（トランザクションシーケンス番号）７０－１－２を「１」としたフレームとなっている。なお、公開鍵認証手順における認証時には、Algorithm Number７０－１－１～７０－４－１は常に

「ｎ」（ｎは「０」又は「１」でない任意の数）であるものと定義する。Algorithm Number７０－１－１～７０－４－１を「ｎ」とすることにより、Shared Key方式による認証手順と区別することが可能となる。

【００６３】ステップＳ６１でＳＴＡ２から公開鍵認証要求を受信したＡＰ１は、認証フレーム６２を用いてＡＰ１の保持するユーザ証明書をＳＴＡ２に対して送信する（ステップＳ６２）。認証フレーム６２は、図７の（２）認証フレーム６２に示す形式となっており、Algorithm Number７０－２－１は前述の通り「ｎ」であり、Transaction Sequence Number ７０－２－２は「２」で、APのユーザ証明書７０－２－３にＡＰ１の保持するユーザ証明書（ユーザ証明書に付随するＡＰ１の公開鍵をも付したもの）を挿入したフレームとなっている。

【００６４】ステップＳ６２でＡＰ１から認証フレーム６２を受信したＳＴＡ２は、ＡＰ１から受信したＡＰ１のユーザ証明書の内容を検証して、ＡＰ１のユーザ証明書の検証結果に問題の無いことを確認すると、ＡＰ１のユーザ証明書に添付された公開鍵を用いて、ＳＴＡ２の保持するユーザ証明書の暗号化を行う（ステップＳ６３）。そして、暗号化したＳＴＡ２のユーザ証明書を、ＳＴＡ２のユーザ証明書に付随するＳＴＡ２の公開鍵と共に、認証フレーム６３を用いてＡＰ１に対して送信する（ステップＳ６４）。認証フレーム６３は、図７の（３）認証フレーム６３に示す形式となっており、Algorithm Number７０－３－１は前述の通り「ｎ」であり、Transaction Sequence Number ７０－３－２は「３」で、APの公開鍵で暗号化したSTA のユーザ証明書７０－３－３を付加したフレームとなっている。

【００６５】ステップＳ６４で認証フレーム６３を受信したＡＰ１は、APの公開鍵で暗号化したSTA のユーザ証明書７０－３－３をＡＰ１の秘密鍵で復号化して、ＳＴＡ２のユーザ証明書の内容を検証し、ＳＴＡ２のユーザ証明書の検証結果に問題の無いことを確認すると、次に今度は共通鍵を生成し、ＳＴＡ２のユーザ証明書に添付された公開鍵を用いて生成した共通鍵を暗号化する（ステップＳ６５）。そして暗号化した共通鍵を、認証フレーム６４を用いてＳＴＡ２に送信し、認証許可を通知する（ステップＳ６６）。認証フレーム６４は、図７の（４）認証フレーム６４に示す形式となっており、Algorithm Number７０－４－１は前述の通り「ｎ」であり、Transaction Sequence Number ７０－４－２は「４」で、STA の公開鍵で暗号化した共通鍵７０－４－３を付加したフレームとなっている。なお、図７に示したStatus Code ７０－１－９、Status Code ７０－２－９、Status Code ７０－３－９及びStatus Code ７０－４－９は、フレーム受信成功の可否などを通信相手に通知するための情報フィールドである。

【００６６】その後、ステップＳ６６でＡＰ１から認証フレーム６４を受信したＳＴＡ２は、STA の公開鍵で暗号化した共通鍵７０－４－３をＳＴＡ２の秘密鍵で復号化して、ＡＰ１が生成した共通鍵を復元し、この後実際に行われる無線通信におけるフレーム暗号化に、該共通鍵を使用することとなる（ステップＳ６７）。以上の動作により、公開鍵認証手順が終了となり、以後、ＳＴＡ２とＡＰ１間でフレーム暗号化通信が行われることとなる。

【００６７】次に、再認証が行われる際の公開鍵再認証手順について、図８及び図９を参照して説明する。

【００６８】図８は、公開鍵再認証手順を示す図であり、図９は、公開鍵再認証手順において送受信されるＭＡＣフレームのフレームボディ部（図３のFrameBody３０－３）を示す図である。

【００６９】図８において、認証要求先のＡＰ１に対して過去に公開鍵認証完了実績のあるＳＴＡ２は、公開鍵再認証要求としてＡＰ１に対して認証フレーム８１を送信する（ステップＳ８１）。認証フレーム８１のフレームボディ部は、図９の（１）認証フレーム８１に示す形式となっており、Algorithm Number（アルゴリズム番号）９０－１－１を「ｍ」とし、Transaction Sequence Number （トランザクションシーケンス番号）９０－１－２を「１」としたフレームとなっている。なお、公開鍵再認証手順における認証時には、Algorithm Number９０－１－１～９０－２－１は常に「ｍ」（ｍは「０」と「１」と「ｎ」でない任意の数）であるものと定義する。Algorithm Number９０－１－１～９０－２－１を「ｍ」とすることにより、図６に示した公開鍵認証手順と区別することが可能となる。

【００７０】ステップＳ８１でＳＴＡ２から公開鍵再認証要求を受信したＡＰ１は、ＡＰ１が保持している図４に示した公開鍵管理テーブル４０において、公開鍵再認証要求を送信したＳＴＡ２のMACアドレスがSTA Mac Address ４０－１に存在するか検索を行う（ステップＳ８２）。そして、検索が成功し、かつ、それに対応する公開鍵をPublic Key４０－２の欄に保持していることを確認した場合には、ＡＰ１は当該ＳＴＡ２に対して指定する共通鍵を新たに生成し、この新共通鍵を公開鍵管理テーブル４０のPublic Key４０－２から取得した公開鍵（当該ＳＴＡ２の公開鍵）を用いて暗号化する（ステップＳ８３）。そして、暗号化した新共通鍵を、認証フレーム８２を用いてＳＴＡ２に送信する（ステップＳ８４）。認証フレーム８２は、図９の（２）認証フレーム８２に示す形式となっており、Algorithm Number９０－２－１は前述の通り「ｍ」であり、Transaction Sequence Number ９０－２－２は「２」で、STA の公開鍵で暗号化した新共通鍵９０－２－３を付加したフレームとなっている。なお、図９に示したStatus Code ９０－１－９及びStatus Code ９０－２－９は、フレーム受信成功の可否などを通信相手に通知するための情報フィールドである。

【００７１】その後、ステップＳ８４でＡＰ１から認証フレーム８２を受信したＳＴＡ２は、STA の公開鍵で暗号化した新共通鍵９０－２－３をＳＴＡ２の保持する秘密鍵で復号化して、ＡＰ１が新たに生成した新共通鍵を復元し、この後実際に行われる無線通信におけるフレーム暗号化に、該新共通鍵を使用することとなる（ステップＳ８５）。以上の動作により、公開鍵再認証手順が終了となり、以後、ＳＴＡ２とＡＰ１間でフレーム暗号化通信が行われることとなる。

【００７２】以上、本発明の第１の実施形態について詳細に説明した。第１の実施形態においては、ＡＰ１とＳＴＡ２が共に自らの秘密鍵とそれに対応する公開鍵、及び公開鍵を添付したユーザ証明書を保持し、当該ユーザ証明書は認証機関に代表される第三者によって公開鍵とその保有者との関係及び保有者自身の正当性を証明可能であるという条件のもとで、ＳＴＡ２がＡＰ１に対して公開鍵認証要求を行い、ＡＰ１から認証許可を得るまでには、図６に示す公開鍵の交換手順が発生するが、本発明に基づき、ＡＰ１とＳＴＡ２が認証完了実績のある相手の公開鍵情報を認証解除後も保持し続けることにより、２回目以降の認証要求時において図８に示す公開鍵再認証手順を用いることにより、初回の認証手順で行ったＡＰ１とＳＴＡ２間での公開鍵交換手順を省略することで、認証処理手順の簡略化が可能となる、という効果を有している。

【００７３】また、図６に示す初回の公開鍵認証手順においてユーザ証明書を用いることにより、ＡＰ１はＳＴＡ２の公開鍵とその保有者であるＳＴＡ２の正当性とを確認した上での認証許可後にＳＴＡ２の公開鍵情報を保持することから、当該ＳＴＡ２のMACアドレスを使用した成りすましによる再認証要求が発生した場合には、図８に示す公開鍵再認証手順を行うＡＰ１は、ＳＴＡ２に対して送信する共通鍵を正当なＳＴＡ２のみが保持する秘密鍵に対応した公開鍵によって暗号化するため、成りすましによる再認証要求元ＳＴＡはこれを復号化し共通鍵を取得することができず、従って本発明によって不正なＳＴＡによる成りすましを防ぐことが可能となる、という効果を有している。

【００７４】次に、本発明の第２の実施形態について説明する。

【００７５】第２の実施形態は、複数のＡＰ（基地局）による複数のＢＳＳ（基本サービス・セット）が存在し、且つ各ＢＳＳ同士が有線又は無線で接続される複合ネットワーク上において、各ＡＰに帰属中のＳＴＡ（移動端末局）に関する公開鍵管理情報（具体的には、図４に示した公開鍵管理テーブル４０）を、複合ネットワーク内における共有情報とする構成とした無線ＬＡＮシステムである。複合ネットワーク内における共有情報とする構成は、例えば、複数のＡＰを統括する上位ＡＰを配設し、上位ＡＰが公開鍵管理情報を一括して保持しておき、各ＡＰは必要時に上位ＡＰに対する登録あるいは問い合わせを行い、その回答を上位ＡＰから得る構成である。このような構成とすることにより、任意ＡＰに帰属中のＳＴＡが、ＢＳＳの移動により他のＡＰへ初回の公開鍵認証を行う際にも、本発明による公開鍵再認証手順を実施することにより認証処理手順の簡略化が可能となる、という効果を有するものとなる。

【００７６】次に、本発明の第３の実施形態について説明する。

【００７７】第３の実施形態は、IEEE802.11で定義するところのIndependent （インディペンデント：独立）方式の無線ＬＡＮシステムに第１の実施形態の本発明を適用する構成である。Independent 方式では、ＩＢＳＳ（Independent BSS ：インディペンデントＢＳＳ）内に複数のＳＴＡだけが存在し、ＡＰは存在しない。そして、ＩＢＳＳ内におけるＳＴＡ間での公開鍵認証時において、本発明の第１の実施形態に基づき、公開鍵認証要求を受信したＳＴＡが認証要求元ＳＴＡの公開鍵管理情報（具体的には、図４に示した公開鍵管理テーブル４０）を保持し続ける構成としたものである。このような構成とすることにより、２回目以降の公開鍵再認証処理手順の簡略化が可能となる、という効果を有するものとなる。

【００７８】なお、本発明の第１、第２及び第３の実施形態において、認証許可を行うＢＳＳ内ＡＰやＩＢＳＳ内ＳＴＡが保持する認証要求元ＳＴＡに関する公開鍵管理情報と共に、ユーザ証明書に基づく有効期限情報を導入することによって、公開鍵管理情報の保持期限を持たせる構成とすることにより、有効期限切れユーザ証明書の継続使用を防ぐことが可能となる。

【００７９】

【発明の効果】以上説明したように、本発明の無線ＬＡＮシステムにおける認証方法と認証装置は、無線通信を行う当事者間でのみ秘匿性を保持した暗号用の鍵配送と認証手順の同時実現を可能とすることができるので、初回の認証を完了したＳＴＡ（移動端末局）に関しては、認証解除後の同一ＡＰ（基地局）に対する２回目以降の認証手順の簡略化を実現可能とする、という効果を有している。

【図面の簡単な説明】

【図１】本発明の無線ＬＡＮシステムにおける認証装置の一実施形態を示すブロック図である。

【図２】ＡＰとＳＴＡの一例を示す詳細ブロック図である。

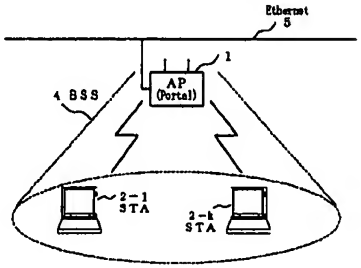
【図３】認証要求時にＡＰとＳＴＡ間で送受信されるＭＡＣフレームの構成を説明する図である。

【図４】ＡＰが保持する公開鍵管理テーブルを説明する図である。

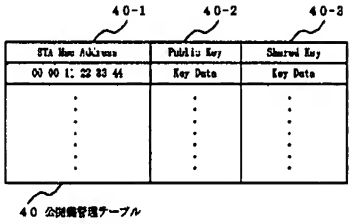
【図６】ＳＴＡが保持するＡＰ情報管理テーブルを説明する図である。

【図６】公開鍵認証手順を示す図である。
【図７】公開鍵認証手順において送受信されるMACフレームのフレームボディ部を示す図である。
【図８】公開鍵再認証手順を示す図である。
【図９】公開鍵再認証手順において送受信されるMACフレームのフレームボディ部を示す図である。
【図１０】Shared Key方式における認証手順を示す図である。
【図１１】Shared Key方式の認証手順において送受信されるフレームフォーマットのフレームボディ部を示す図である。
【符号の説明】
1　AP
2　STA
4　BSS
5　Ethernet（イーサネット）
１２　無線機部
１３　IEEE802.11 PHYプロトコル処理部
１４　IEEE802.11 MACプロトコル処理部
１５　上位レイヤ処理部
１６　メモリ
１７　上位レイヤインターフェース
１８　基地局端末本体
１９　無線ＬＡＮカード
２０　移動端末本体

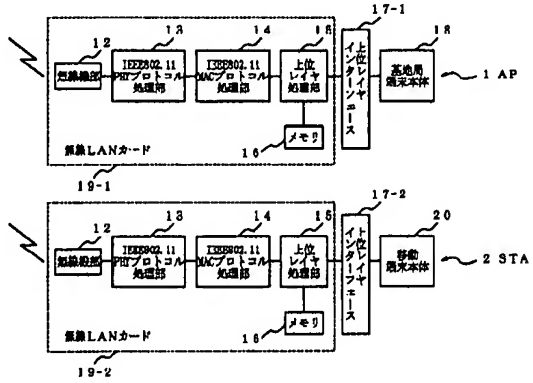
【図１】



【図４】

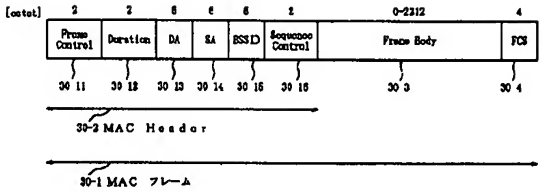


【図２】

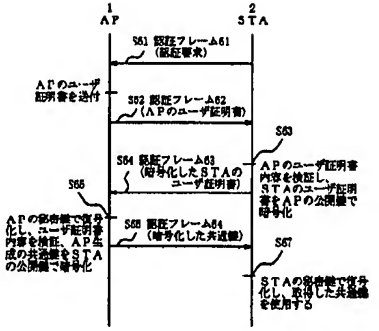


【図５】

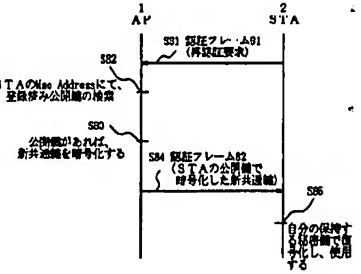
【図３】



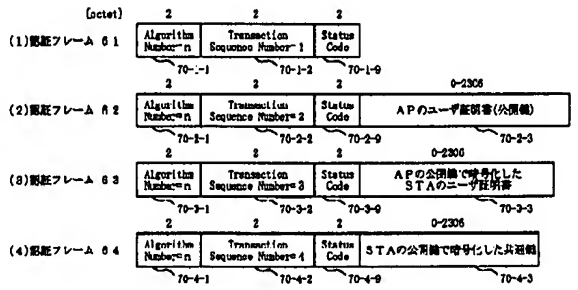
【図６】



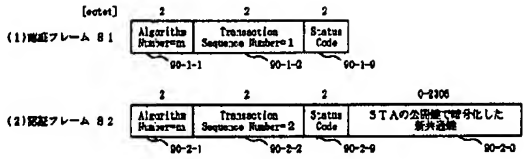
【図８】



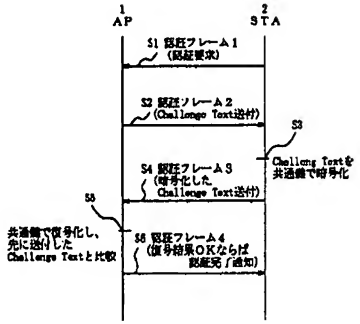
【図７】



【図9】



【図10】



【図11】